

普通高等学校本科专业设置申请表

校长签字:

学校名称(盖章): 浙江理工大学

学校主管部门: 浙江省

专业名称: 网络空间安全

专业代码: 080911TK

所属学科门类及专业类: 工学 计算机类

学位授予门类: 工学

修业年限: 四年

申请时间: 2025-07-18

专业负责人: 沈剑

联系电话: 13382769420

教育部制

1. 学校基本情况

学校名称	浙江理工大学	学校代码	10338
主管部门	浙江省	学校网址	www.zstu.edu.cn
学校所在省市区	浙江杭州下沙高教园区 2号大街928号	邮政编码	310018
学校办学基本类型	☐ 教育部直属院校 ☐ 其他部委所属院校 ☒ 地方院校		
	☒ 公办 ☐ 民办 ☐ 中外合作办学机构		
已有专业学科门类	☐ 哲学 ☒ 经济学 ☒ 法学 ☐ 教育学 ☒ 文学 ☐ 历史学 ☒ 理学 ☒ 工学 ☐ 农学 ☐ 医学 ☒ 管理学 ☒ 艺术学		
学校性质	☒ 综合 ☐ 理工 ☐ 农业 ☐ 林业 ☐ 医药 ☐ 师范 ☐ 语言 ☐ 财经 ☐ 政法 ☐ 体育 ☐ 艺术 ☐ 民族		
曾用名	浙江丝绸工学院 浙江工程学院		
建校时间	1897	首次举办本科教育年份	1959年
通过教育部本科教学评估类型	审核评估	通过时间	2025年06月
专任教师总数	1911	专任教师中副教授及以上职称教师数	974
现有本科专业数	68	上一年度全校本科招生人数	4793
上一年度全校本科毕业生人数	4407		
学校简要历史沿革	我校前身蚕学馆1897年创办，是我国最早的新学教育机构之一。1908年升格为高等蚕桑学堂。1959年开始招收本科生，1983年获硕士学位授予权，2006年获博士学位授予权。1964年定名为浙江丝绸工学院，1999年更名为浙江工程学院，2004年更名为浙江理工大学。2017年入选浙江省重点建设高校。		
学校近五年专业增设、停招、撤并情况	2021年，新增大数据管理与应用专业，电子商务专业停止招生。撤销广告学专业。 2022年，新增服装与服饰设计、数字媒体艺术专业。 2023年，无变化。 2024年，新增软件工程、艺术与科技、能源化学工程专业，数字媒体技术专业停止招生。撤销材料成型及控制工程、公共事业管理专业。 2025年，材料化学、电气工程及其自动化、海洋资源开发技术、风景园林专		

	业停止招生。撤销包装工程专业。
--	-----------------

2. 申报专业基本情况

申报类型	新增国控专业		
专业代码	080911TK	专业名称	网络空间安全
学位授予门类	工学	修业年限	四年
专业类	计算机类	专业类代码	0809
门类	工学	门类代码	08
申报专业类型	新建专业	原始专业名称	-
所在院系名称	信息科学与工程学院(网络空间安全学院)		
学校现有相近专业情况			
相近专业1专业名称	-	开设年份	-
相近专业2专业名称	-	开设年份	-
相近专业3专业名称	-	开设年份	-

3. 申报专业人才需求情况

申报专业主要就业领域	网络空间安全专业毕业生经过四年的学习，具有了扎实的理论基础、坚实的专业知识和优秀的道德品质，因此可在以下几个领域就业： (1)可从事安全信息服务：为政府、国防、军队、电信、电力、金融、铁路等部门的网络与信息安全领域进行管理、科研与服务。 (2)可从事安全技术研发：到国内外大型电信服务商、大型通信设备制造企业、国内外众多软件企业、国家机关以及各个大中型企事业单位的信息技术部门、教育部门进行安全技术的研究、设计、开发、维护和教育培训等工作。 (3)可继续进一步学业深造：继续攻读计算机科学与技术、网络空间安全、网络工程、通信、信息处理、软件工程和其他相关学科的硕士学位。
人才需求情况	网络空间安全是关乎国家安全和发展的重大战略问题。2003年《国家信息化领导小组关于加强信息安全保障工作的意见》被颁发。2013年11月12日成立中央国家安全委员会。2014年2月27日成立中央网络安全和信息化领导小组，同时，“维护网络安全”首次列入政府工作报告。国家《国民经济和社会发展的第十四个五年规划和2035年远景目标纲要》中明确提出，要全面加强网络安全保障体系和能力建设，加强网络安全宣传教育和人才培养。

	1、国防建设对网络空间安全高层次人才的需求 习近平总书记在2014年中央网络安全和信息化领导小组第一次会议上的讲话指出“没有网络安全就没有国家安全”。中央军委印发了《关于进一步加强军队信息安全工作的意见》，明确强调了“扎实抓好网络空间安全防护力量建设，为网络空间安全建设管理提供人才支撑”。党的二十大报告进一步指出“提高公共安全治理水平，加强个人信息保护”，对网络空间安全相关专业领域的建设和人才的培养提出了更高的要求。 2、国家互联网经济建设对网络空间安全高层次人才的需求 2022年的《中国互联网络发展状况统计报告》显示，互联网推动网民消费模式变迁。2015年12月我国网络支付用户规模达4.16亿，截止2022年6月我国网络支付用户规模达9.04亿。消费模式的变迁同样带来巨大的挑战，对信息的安全性、保密性、可用性等提出高要求。网络空间的安全威胁来自安全漏洞，其中又以未公开漏洞为主要威胁。随着网络支付与无接触支付越来越普及，信息技术成为重要安全保障。国家的网络强国建设、国民新型消费都需要网络空间安全专业知识团队的支撑。 3、网络空间安全产业建设对网络空间安全高层次人才的需求 2021年全球网络安全相关硬件、软件、服务总投资规模达到1687.7亿美元，预计在2026年增至2875.7亿美元，五年复合增长率（CAGR）将达11.3%。聚焦中国市场，2026年中国网络安全IT支出规模将达到318.6亿美元，全球占比约为11.1%，五年CAGR约为21.2%。中国网络安全市场增速持续领跑全球，五年CAGR近全球两倍，市场前景广阔。社会对网络空间安全的人才需要量大约为每年增加1.2万人左右。在“十四五”规划下，未来五年网络空间安全市场会跟随国家整体科技进步的方向快速发展，随着网络空间安全市场越来越大，对于网络空间安全专门人才需求量急剧增加。	
申报专业人才需求调研情况	年度招生人数	35
	预计升学人数	20
	预计就业人数	15
	杭州海康威视数字技术股份有限公司	5
	杭州安恒信息技术股份有限公司	3
	新华三信息安全技术有限公司	2
	博智安全科技股份有限公司	2

	浙江大华技术股份有限公司	2
	浙江凌迪数字科技有限公司	1

4. 产业调研报告

网络空间安全专业产业调研报告

一、调研工作组织与实施情况

2025 年数字化转型加速、网络安全威胁加剧，本次调研旨在洞察网络空间安全专业发展态势及行业需求变化。通过调研国防、互联网经济等领域用人单位，收集师生、企业反馈，剖析三所对标高校培养方案，明确网络空间安全人才培养方案制订思路。以期掌握行业对人才知识、技能、素质的最新需求，优化课程体系与实践教学，提升学生竞争力，输送契合行业需求的高素质人才，推动专业创新发展。

(1) 调研目的与意义

旨在深入了解网络空间安全专业人才市场的需求，分析行业在国防安全、互联网经济、产业发展等领域的发展趋势，以及现有教育模式与实际需求之间的差距。通过调研，可以为网络空间安全专业本科人才培养方案的制订提供科学依据，确保教育内容与国家网络安全战略、社会实际需求及产业发展走向相匹配，提高人才培养的质量和针对性。

(2) 调研内容

调研网络空间安全行业在国防建设、互联网经济、产业发展等领域的现状与趋势，明确不同领域对人才在 AI 安全等前沿知识掌握、新型攻击防御等技能水平、安全意识等职业素养的要求。评估现有课程与相近专业的差异化，及课程体系覆盖核心领域的全面性、教学方法与实践环节的有效性。收集毕业生就业数据，分析其就业去向、职业发展及对专业培养的反馈。调研校企合作现状与成效，探索创新合作模式以促进产教融合。

(3) 调研方法

文献调研：收集和分析国内外网络空间安全专业教育的相关资料，包括教育政策、课程标准、教学方法、行业发展报告等。

问卷调查：设计问卷，通过网络和实地发放，收集学生、教师、企业等多方面的意见和需求，涵盖课程设置、实践教学、行业需求等内容。

访谈：对网络空间安全行业专家、企业技术负责人、教育工作者等进行深入访谈，获取一手信息。

案例研究：选择具有代表性的网络空间安全领域企业和教育机构，进行案例分析，总结成功经验和存在的问题。

(4) 调研组织

成立调研小组：由网络空间安全领域教育专家、行业专家、教师代表和学生代表组成，负责调研的组织和实施。

明确分工：根据调研内容，将调研小组分为文献分析组、问卷设计与发放组、访谈组、案例研究组等不同工作组，明确各自的职责和任务。

制定调研计划：制定详细的调研计划，包括调研时间、地点、对象、方法等，涵盖国防单位、互联网企业、对标高校等调研场景。

(5) 调研实施

前期准备：进行调研培训，确保调研人员了解调研目的、方法和注意事项，熟悉网络空间安全专业前沿知识，准备好问卷、访谈提纲等工具。

实地调研：按照调研计划，开展实地调研，前往国防领域单位、互联网企业、北京航空航天大学、武汉大学、暨南大学等对标高校收集数据和信息。

数据处理：对收集到的数据进行整理和分析，形成初步的调研报告。

结果反馈：将调研结果反馈给相关利益相关者，征求意见和建议，完善调研报告。

(6) 调研成果应用

人才培养方案制订：根据调研结果，细化完善网络空间安全专业本科人才培养方案，优化课程体系，强化前沿技术相关课程。

教学改革：推动教学内容、方法和实践环节的改革，引入行业最新技术案例，采用多样化教学方法，提升学生实践能力。

校企合作深化：根据调研结果，深化校企合作，探索“订单式”人才培养、共建产业学院等模式，促进产教融合，为培养方案制订提供具体思路。

二、本专业发展现状及趋势

调研/对标高校	调研专业	培养方案优势和特色
		优势：1. 学科底蕴深厚，拥有网络空间安

北京航空航天大学	网络空间安全	全一级学科博士点、博士后流动站，入选国家“双一流”建设学科，依托国家级网络空间安全实验室构建“基础研究 - 技术研发 - 工程应用”完整培养链。 实战能力培养突出，开设“网络空间安全综合实战”系列课程（共 5 学分）和 4 学分的科研创新实践，学生参与“强网杯”“全国大学生信息安全竞赛”等国家级赛事获奖率连续三年位居全国前 5%。 特色：1. 分设“空天网络安全”“人工智能安全”“密码理论与技术”3 个模块方向，开设《空天信息网络安全》《量子密码技术》《AI 安全风险与防护》等前沿课程。 2. 与航天科技集团、奇安信等共建“网络安全联合实验室”，年均承接 20 余项国家级网络安全保障项目（如国家重大活动网络防护、航天系统安全检测），学生实战参与度超 70%。
武汉大学	网络空间安全	优势：1. 跨学科融合鲜明，要求跨学科基础选修课 3 学分（涵盖法学、大数据、通信等领域，如《法学导论》《大数据分析基础》）、跨专业选修课 5 学分（如《区块链技术原理与安全》），培养“技术 + 法规 + 管理”复合型安全人才。 实践教学体系完善，集中实践共 35 学分，含“网络安全科研训练与论文写作”“国家级

		网络应急响应演练”等特色模块，依托国家级网络空间安全实验教学示范中心开展沉浸式教学。 特色：1. 分设 “数据安全与隐私保护” “网络攻防与应急响应” 两个专业方向，开设《数据安全法实务》《网络安全态势感知与预警》《隐私计算工程实践》等课程。 2. 注重职业素养与学术衔接，开设 2 学分的 “网络安全伦理与合规” 和 3 学分的 “安全学术前沿论坛”，定期邀请院士、行业首席科学家开展专题授课，年均举办 15 场以上高水平学术讲座。
暨南大学	网络空间安全	优势：1. 实践学分占比高，实践教学共 36 学分（占总学分 25%），含 “网络安全攻防实战进阶” “安全产品开发与落地实践” 等特色环节，依托粤港澳网络空间安全协同创新中心构建 “课 - 赛 - 研 - 产” 一体化实践平台。 2. 产业对接紧密，限选课程 “网络安全产业应用与管理” 聚焦技术商业化能力，与华为、腾讯、深信服等共建 “大湾区网络安全联合实验室”，年均引入企业真实项目 30 余个用于教学。 特色：1. 突出 “安全 + 区域产业” 交叉特色，开设《粤港澳大湾区网络安全治理》《跨境数据安全合规》《安全产品运营与市场

		分析》等课程，贴合大湾区数字经济发展需求。 2. 创新创业教育成效显著，开设 “网络安全创新创业工坊” 课程（3 学分），联合孵化器年均孵化 5-8 个学生安全技术创业项目，近三年获 “互联网 +” “挑战杯” 等国家级创新创业赛事奖项 12 项。
--	--	--

1、国内外现状及发展趋势

国内现状及发展趋势

近年来，我国网络空间安全领域呈现加速发展态势，已成为保障国家安全和数字经济发展的核心支撑。国家层面高度重视网络安全建设，从 2003 年《国家信息化领导小组关于加强信息安全保障工作的意见》到 “十四五” 规划中 “全面加强网络安全保障体系和能力建设” 的明确部署，形成了完善的政策支撑体系。党的二十大报告进一步提出 “提高公共安全治理水平，加强个人信息保护”，将网络空间安全提升至国家战略高度。

从产业发展看，中国网络安全市场增速持续领跑全球，IDC 数据显示，2026 年中国网络安全 IT 支出规模预计达 318.6 亿美元，五年复合增长率达 21.2%，近全球两倍。随着 5G、云计算、人工智能、区块链等技术的广泛应用，网络安全的应用场景不断拓展，从传统网络防护向工业互联网安全、云计算安全、数据安全等细分领域延伸。但人才供给严重不足，据《网络安全人才实战能力白皮书》，我国网络安全人才缺口超 140 万，每年高校培养人才仅 3 万余人，预计 2027 年缺口将扩大至 300 万，人才培养已成为行业发展的关键瓶颈。

在技术应用层面，我国网络安全技术快速迭代，在密码学、云计算安全、大数据安全等领域形成了一批具有自主知识产权的技术成果。我校已建成全省数字时尚与数据治理重点实验室，与海康威视共建智能物联网络与数据安全重点实验室，推动 “多媒体大数据安全” “云计算安全” 等技术落地应用，同时通过教育部产学研合作协同育人项目，加速教育与产业需求的对接。

国际现状及发展趋势

全球网络空间安全已进入 “高威胁、高投入、高竞争” 的新阶段，网络安

全作为非传统安全因素，与政治安全、经济安全等深度融合。以美国为代表的发达国家在网络安全领域布局较早，2009 年美军成立网络司令部，构建了专业化网络作战力量；美国国家安全局（NSA）在网络攻击技术研发、全球网络监控等方面持续领先，2022 年针对西北工业大学的网络攻击事件即显示其成熟的网络战能力。

从市场规模看，2021 年全球网络安全相关投资达 1687.7 亿美元，预计 2026 年增至 2875.7 亿美元，五年复合增长率 11.3%。国际网络安全企业在零信任架构、威胁情报、量子加密等前沿领域占据技术优势，同时人工智能驱动的自动化攻击、供应链安全威胁等新型风险持续涌现，推动全球网络安全技术向智能化、协同化方向发展。

国际合作与竞争并存，各国一方面加强网络安全领域的技术交流，另一方面也在关键技术和人才领域展开激烈竞争。欧盟通过《通用数据保护条例》（GDPR）建立了严格的数据安全规范，影响全球数据治理规则；美国则通过“清洁网络”等计划强化技术壁垒，网络空间安全已成为大国科技竞争的核心领域之一。

综上所述，网络空间安全专业的国内外发展呈现“政策驱动强劲、技术迭代加速、人才需求迫切”的共同特征。国内市场在政策红利和数字经济发展推动下，展现出远超全球的增长潜力，但需弥补人才供给短板；国际领域技术竞争与安全威胁并存，要求专业教育既要紧跟全球技术前沿，又要立足国家战略需求，培养具备实战能力、国际视野和家国情怀的复合型人才。未来，随着量子计算、人工智能等技术与网络安全的深度融合，专业人才培养需在课程体系、实践教学等方面持续创新，以应对日益复杂的网络安全挑战。

2、调研/对标高校可供借鉴的经验

1) 课程体系的前沿性：通过对北京航空航天大学、武汉大学、暨南大学的调研，发现三所高校在网络空间安全专业课程设置上，紧密锚定国家战略与产业前沿动态。北京航空航天大学聚焦空天领域安全需求，开设《空天飞行器网络安全防护》《量子密码技术》等前沿课程，其“网络空间安全综合实战”系列课程（共 5 学分）直接对接航天系统安全检测等国家级项目，学生通过赛事备赛训练（如“强网杯”）强化实战能力。武汉大学紧扣数据安全与学术前沿，设

置《网络安全态势感知与预警》《隐私计算工程实践》等课程，依托国家级网络空间安全实验教学示范中心，将“国家级网络应急响应演练”纳入实践环节，确保课程内容与技术发展同步。暨南大学贴合大湾区数字经济特点，开设《跨境数据安全合规》《安全产品运营与市场分析》等特色课程，通过“课 - 赛 - 研 - 产”一体化平台，将企业真实安全项目（年均 30 余个）融入“网络安全攻防实战进阶”课程，强化前沿技术落地能力培养。

2) 学科的融合性：为培育复合型人才，三所高校在课程设计中强化多学科交叉融合：北京航空航天大学开设《网络安全伦理与空天合规》课程，通过与航天科技集团共建的“网络安全联合实验室”，推动空天技术与安全防护知识的跨领域应用，其“网络安全前沿技术工坊”课程涵盖安全技术向航天领域转化的市场化分析内容。武汉大学明确跨学科基础选修课 3 学分（如《法学导论》《大数据分析基础》）、跨专业选修课 5 学分（如《区块链技术原理与安全》），通过“跨学科科研训练”项目引导学生融合技术与法律知识开展研究，同时精简传统理论课程学时（如“网络安全基础”压缩至 3 学分，增加案例教学占比）。暨南大学突出产业与安全的交叉融合，开设《大湾区数字经济安全治理》等课程，其“网络安全产业应用与管理”限选课程邀请华为、腾讯等企业导师授课，强化产业思维；通过“网络安全创新创业工坊”课程（3 学分），将安全技术与商业运营知识结合，在总学时限制下，通过优化教学方法确保核心知识点高效传递。

三、利益相关方调研情况

通过对专业师生、用人单位和毕业生开展问卷调查和访谈，结合网络空间安全专业特点及相关合作单位情况，得出以下主要结论：

1. 专业师生

多数师生认为现有与网络空间安全专业相关的课程体系框架基本合理，涵盖密码学、计算机网络安全等核心内容，但希望进一步增加大数据安全、AI 安全防护等前沿技术课程比重，同时强化实战化教学环节。学生普遍反映网络攻防演练、真实漏洞挖掘等实践机会较少，期待与企业共建的安全靶场、联合实验室能提供更多沉浸式实践场景。针对以上反馈，拟通过新增前沿课程、扩容企业实践

项目等方式优化。

2. 用人单位

合作用人单位（如杭州海康威视数字技术股份有限公司、博智安全科技股份有限公司、北京信安世纪科技股份有限公司等）反馈，毕业生具备扎实的网络安全理论基础，但在复杂场景下的应急响应、安全架构设计等实战能力需进一步提升。博智安全科技股份有限公司建议加强跨学科融合，增设网络安全与法律、安全产品运营等交叉课程，强化复合型人才培养；北京信安世纪科技股份有限公司提出，需强化对密码技术应用、零信任安全架构等核心领域的深度教学，提升学生在商用密码产品开发、安全协议设计等方面的专业能力。针对以上反馈，将通过增加交叉课程、细化专业方向、强化核心领域实战训练等方式改进。

3. 相关高校毕业生

武汉大学、暨南大学和北京航空航天大学网络空间安全专业的毕业生普遍认可在校期间学习的密码编码学、网络攻防技术等课程对职业发展的支撑作用，但部分反馈部分课程内容更新滞后于产业发展，例如传统密码算法教学占比过高，而区块链安全、隐私计算等新兴技术的教学内容不足。多位在安全企业任职的毕业生提到，实际工作中面临的自动化攻击防御、供应链安全检测等新型挑战，需要学校加强前沿技术动态跟踪与教学融入。针对以上反馈，将加快课程内容更新，增加新兴技术教学模块。

四、本科人才培养方案制定思路及具体举措

通过以上调研和分析，本科人才培养方案制订思路如下：

1. 紧密贴合网络安全行业动态，大力引入大数据安全、安全攻防等前沿技术课程，并持续更新现有课程内容，确保知识体系与时俱进。
2. 进一步强化实践教学环节，深化与海康威视、博智安全科技等合作单位的产教融合，共建实训基地，开展实战化项目训练，全面提升学生实践创新能力。
3. 优化课程体系架构，加强网络安全与法学、管理学等跨学科融合，增设网络安全合规、安全运营管理等课程，强化学生综合素质培养。

主要具体举措如下：

1. 优化专业方向选择机制，要求学生在通信安全、物联网安全两大模块中择

一修读，细化专业能力培养路径。

2. 在实践教学环节新增网络安全应急响应实训、网络攻防加固实践两门实践选修课，增强学生实操技能。

3. 因总学时限制，部分课程学时与学分适度压缩，通过优化教学方法，确保核心知识点有效传递。

4. 深化校企合作融入教学内容，在网络安全专业实习、安全项目综合实践等环节，引入企业真实安全项目，如参与企业安全运维、漏洞检测等工作，提升学生解决实际问题的能力。

工作组组长（签字）： 李金润

领导小组组长（签字）： 

2025 年 7 月 20 日

5. 申请增设专业人才培养方案

网络空间安全专业本科人才培养方案

(专业代码: 080911TK)

一、专业名称: 网络空间安全

专业代码: 080911TK

二、培养目标

贯彻落实党和国家的教育方针, 坚持立德树人, 根据国家战略和社会经济发展的需求, 结合行业特色, 培养具有良好科学素质、人文素养、社会责任感、职业道德等德、智、体、美、劳全面发展; 具有扎实的数理和网络空间安全基础理论知识和专业技能; 具有分析、设计、加固、组建、编制、运维安全网络与信息系统的能力; 具有较强的开拓创新意识、团队合作意识、工程实践能力和组织管理能力; 具有国际交流能力、终身学习能力、强烈事业心和担当精神的安全专业高素质人才。

毕业生工作五年后, 可成为信息类、安全类、计算机类等领域内企事业单位的精英人才、技术骨干或项目主管, 在社会和专业领域应具备:

培养目标 1: 能综合运用数理基础知识和网络空间安全领域的基础理论与专业知识, 对网络与信息安全项目、产品或系统的分析和设计过程体现创新意识。

培养目标 2: 能承担网络与信息安全工程中计算机网络、软件工程、信息与通信等领域的安全设计、研发、实施和运行等工作, 能胜任工程师岗位或履行相应职责。

培养目标 3: 具备健全人格、良好的人文科学素养和强烈的社会责任感, 具备职业道德, 能够从法律、伦理、经济、社会和环境等系统视角对安全工程项目进行决策和管理。

培养目标 4: 能与国内外同行、专业客户和社会公众进行有效沟通, 能够融入团队的工作并发挥骨干作用。

培养目标 5: 具有终身学习的能力, 具备开阔的国际视野, 能及时跟踪网络空间安全专业领域的技术发展动态, 服务网络与信息安全领域的创新发展和产业升级, 具备职业竞争能力。

三、毕业要求

本专业学生主要学习网络空间安全方面的基本理论、基础知识，接受从事网络空间安全研究与应用的创新训练，具有研究、设计、开发安全应用系统的基本能力。

依据中国工程教育专业认证协会《工程教育认证标准》，毕业生应具备素养、知识和能力等方面的要求：

毕业要求 1. 工程知识：具备较扎实的数学、自然科学知识，系统掌握网络空间安全领域的工程基础和专业基础知识，了解国防领域背景知识，能够将各类知识用于解决计算机领域内的复杂安全工程问题。

毕业要求 2. 问题分析：能够应用数学、自然科学和工程科学的基本原理，识别、表达、并通过文献研究分析网络空间安全及相关领域内的复杂工程问题，以获得有效结论。

毕业要求 3. 设计/开发解决方案：能够设计针对计算机领域复杂安全工程问题的解决方案，设计满足特定需求的软硬件系统、模块或算法流程，并能够在设计环节中体现创新意识，考虑社会、健康、安全、法律、文化以及环境等因素。

毕业要求 4. 科学研究：能够基于计算机领域网络空间安全基础并采用科学方法对复杂的计算机软硬件及系统工程的安全问题进行研究，包括设计实验、分析与解释数据、并通过信息综合得到合理有效的结论。

毕业要求 5. 使用现代工具：能够针对计算机领域内的复杂安全工程问题，选择与使用恰当的安全技术、软硬件及系统资源、先进研发工具和信息技术工具，包括对安全问题的预测与模拟，并能够理解其安全局限性。

毕业要求 6. 工程与社会：能够基于网络空间安全领域背景知识进行合理分析，评价网络空间安全工程实践和复杂工程问题解决方案对社会、健康、安全、法律以及文化的影响，理解应承担的责任。

毕业要求 7. 环境和可持续发展：能够理解和评价针对网络空间安全领域复杂工程问题的专业工程实践对环境、社会可持续发展的影响。

毕业要求 8. 职业规范：具有良好的人文社会科学素养、社会责任感，能够在网络空间安全实践中理解并遵守工程职业道德和规范，履行责任。

毕业要求 9. 个人和团队：能够在多学科背景下的团队中承担个体、团队成员以及负责人的角色。

毕业要求 10. 沟通：能够就计算机领域内的复杂安全工程问题与业界同行及社会公众进行有效沟通和交流，包括撰写报告和设计文稿、陈述发言、清晰表达或回应指令。并具备一定的国际视野，能够在跨文化背景下进行沟通和交流。

毕业要求 11. 项目管理：理解并掌握网络空间安全领域工程管理原理与经济决策方法，并能在多学科环境中应用。

毕业要求 12. 终身学习：具有自主学习和终身学习的意识，有不断学习和适应计算机技术快速发展的能力。

体质健康标准测试必须达标。

毕业要求与培养目标支撑关系表

毕业要求	培养目标1	培养目标2	培养目标3	培养目标4	培养目标5
1. 工程知识	√	√		√	√
2. 问题分析	√	√			
3. 设计/开发解决方案	√	√			
4. 研究		√			√
5. 使用现代工具	√	√			
6. 工程与社会		√	√	√	
7. 环境和可持续发展			√		√
8. 职业规范			√	√	
9. 个人和团队			√	√	√
10. 沟通				√	√
11. 项目管理	√		√	√	
12. 终身学习		√			√

四、主干学科

网络空间安全

五、核心课程

信息论、密码编码学、离散数学、数据结构、计算机组成与系统结构、计

计算机网络、操作系统、

六、学习年限

学制：四年 学习年限：3-6 年 最低毕业学分：164+5 授予学位：工学学士

七、培养方案学分分配（本表格内容待教学计划表确认后再计算填写）

类别	必修	选修	合计	比例	第二课堂
通识教育	59	14	73	44.51%	5
学科（专业）基础教育	18	0	18	10.96%	
专业教育	7	28	35	21.34%	
实践教学环节	28	10	38	23.19%	
其中：实践教学环节(含课内实验教学)			55.6	33.90%	
合 计	112	52	164	100.00%	

八、专业特色

本专业坚持教学和科研相结合，始终贯彻理论与实践并重的育人理念，并注意与国内外同类顶尖院校的合作交流，形成“通识-专业-实践”兼顾的办学特色，立足网络空间安全技术，构建了通信安全、物联网安全两个模块，并在此基础上注重培养学生的软硬件开发能力。依托实践教学基地，充分利用资源优势，为浙江省和国家经济建设服务，培养具有创新意识和较强实践能力的网络空间安全人才。

九、说明

1、体质健康标准测试：学生每学年测试一次（五年制学生只参加前四年测试），具体测试时间、内容、测试方式，成绩评定等可参见《学生手册》中《浙江理工大学关于落实<国家学生体质健康标准>实施办法》文件。

2、第二课堂 5 学分中，其中 2 学分必须为劳动实践相关活动项目。根据《浙江理工大学本科生第二课堂学分管理办法》(浙理工教〔2019〕55 号)的认定项目分类，劳动实践相关活动包括科研活动、学科竞赛、课外实验、社会实践、社团活动、学生活动、“三创”实践专项。鼓励学生在获取第二课堂学分时，积极参加各类农村扶贫开发、城市社区建设、环境保护等各项志愿者活动，文化科技卫生“三下乡”及其他社会实践活动，在劳动中感悟、锤炼、体验。

3、创新创业教育：

(1) 创新创业教育主要依托课程为：创业基础

(2) 设置创新创业模块选修课程，共 6 个学分。该模块课程的学分经认定后可替代相应类别的选修课程学分。创新创业模块选修课程学分由启新学院、创业学院认定。

4、本专业与电子信息工程专业一起，统一按电子信息类招生。在第一学年采用平台教育，课程安排一致，从大二开始进行分专业教育。

网络空间安全专业课程与毕业要求对应关系表

毕业要求 课程名称	要求 1	要求 2	要求 3	要求 4	要求 5	要求 6	要求 7	要求 8	要求 9	要求 10	要求 11	要求 12
中国近现代史纲要								H				L
思想道德与法治							H	H				H
毛泽东思想和中国特色社会主义理论体系概论							H	H				
马克思主义基本原理						H		H				
习近平新时代中国特色社会主义思想概论						H	H	H				
体育									L			L
英语										H		H
大学生心理健康教育						H		M				
身体素质课 1-2								M				L
劳动教育						H		M				
高等数学 A	H	H										
程序设计基础课程设计	M	M			H							
通识选修课						M	M	M				
普通物理 A	H	L										
普通物理实验 B				H								
计算机导论	M					H				M		H
离散数学	M	H		H								
数据结构		H	H	H								
计算机组成与系统结构		H	H	H								L
C 程序设计	H				H							H
C++程序设计	M	L			M							
JAVA 程序设计	M	L			M							
数字电子技术	H	H					L					
计算机网络	M	H	H									L
操作系统	M	H	H	M								
算法设计与分析		H	H	H								
算法与数据结构	M	M									M	
军事技能								L				M
社会实践						H				H		
劳动教育实践						H		H				

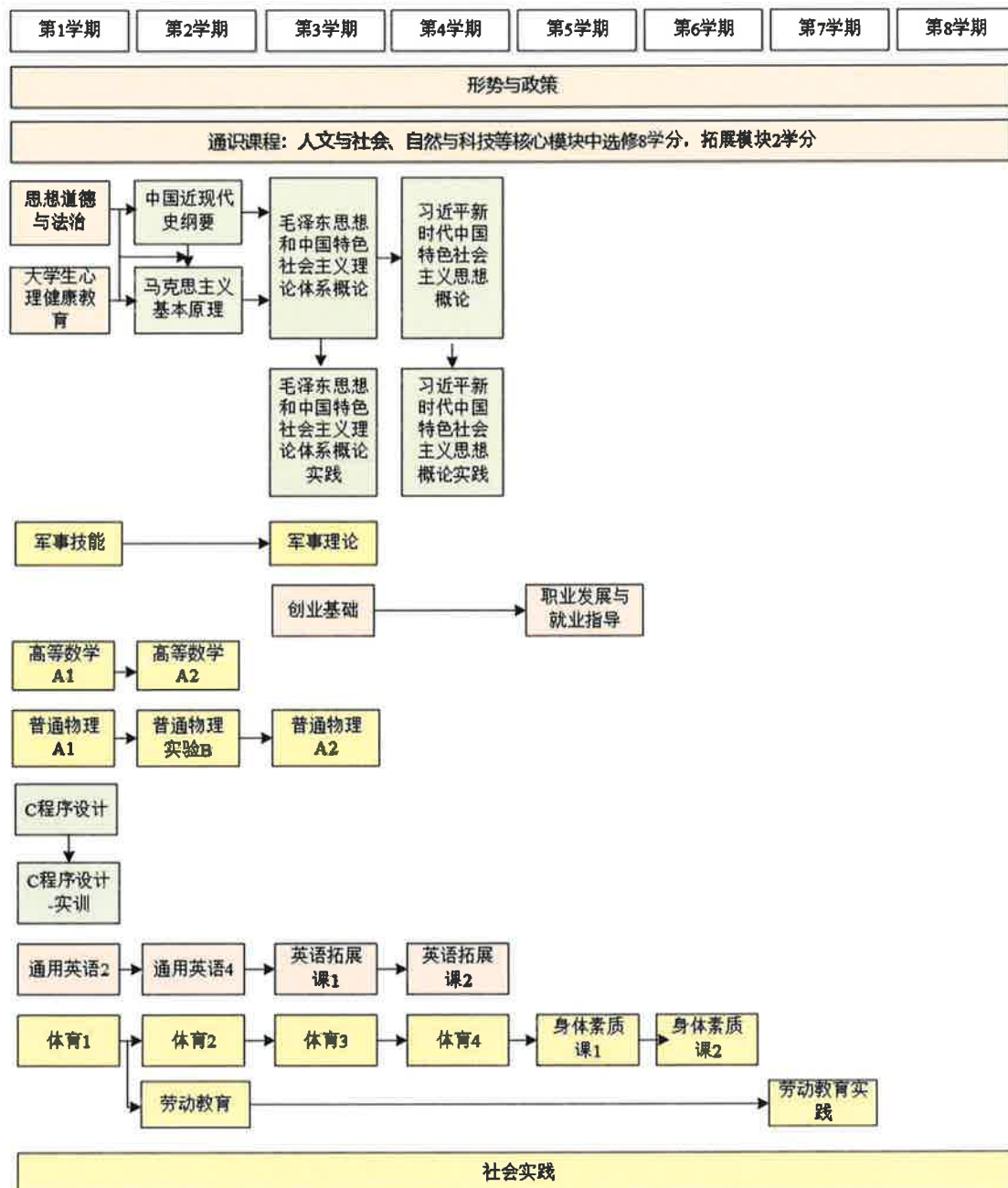
课程名称 \ 毕业要求	要求 1	要求 2	要求 3	要求 4	要求 5	要求 6	要求 7	要求 8	要求 9	要求 10	要求 11	要求 12
安全联合基地实习					M	M						
形势与政策										H		
英语拓展课										H		M
军事理论								H				
职业发展与就业指导						L		H		M	H	
创业基础						H					H	
信息安全数学基础	H	H	L	H	L							
Python 程序设计	M		H		H							H
通信工程导学*	H	H		M	L							
模拟电子技术	H	H		M	M							
网络攻防技术	M	H		H					L			
电磁场与电磁波	H	H					M					
电磁场与电磁波实验				M	L							
C 程序设计-实训	M		H		H							
基于 FPGA 的数字系统设计	L	L			M							
计算机图像处理*		M	L		L							
计算机组成与系统结构课程设计	L				H					H	H	
大数据技术课程设计		H	M		H				H	H	H	
通信电子线路	L	H		L								
操作系统课程实验		M	H	M						H		L
通信原理 A	H	H		H								H
信息论	M	H										
计算机网络安全	H		H									M
计算机网络安全实验				M	M							
密码编码学	M		L									
无线网络安全	M		M	L								
多媒体信息安全	M	L										
云计算安全技术*	M		M							M		
区块链技术		M	L									
数据结构课程实验		M	H	M						H		L
计算机网络课程设计			H		H	H				M		
物联网工程概论	M					L			L			
算法设计与分析实验		H	H		H				M	M		

课程名称 \ 毕业要求	要求 1	要求 2	要求 3	要求 4	要求 5	要求 6	要求 7	要求 8	要求 9	要求 10	要求 11	要求 12
物联网安全技术			M		L							
大数据技术		L	L		M							
通信原理课程设计		M	H		H				M	M		
Python 程序课程设计		H	H		H				M			
算法与数据结构课程设计		M	H		H				M			
通信电子线路实验				H	H							
毕业设计(论文)			H				H			H	H	
区块链技术课程设计		M	H		H							
物联网安全技术课程设计	L	M	H		H				H	H		
工程认识实习						H	H	H				
网络空间安全专业实习						H	M	H			H	
C++程序课程设计			M		L				L	L		
JAVA 程序课程设计			M		L						L	
信息论课程设计	H	H	H						M	M	M	
网络攻防技术实验				M	L	L						
密码编程学综合实验					L	M						
物联网课程设计						L			M	M		
基于 FPGA 的数字系统设计实践	M	M	H	L	H				H			
无线网络安全课程设计	M	H		M								

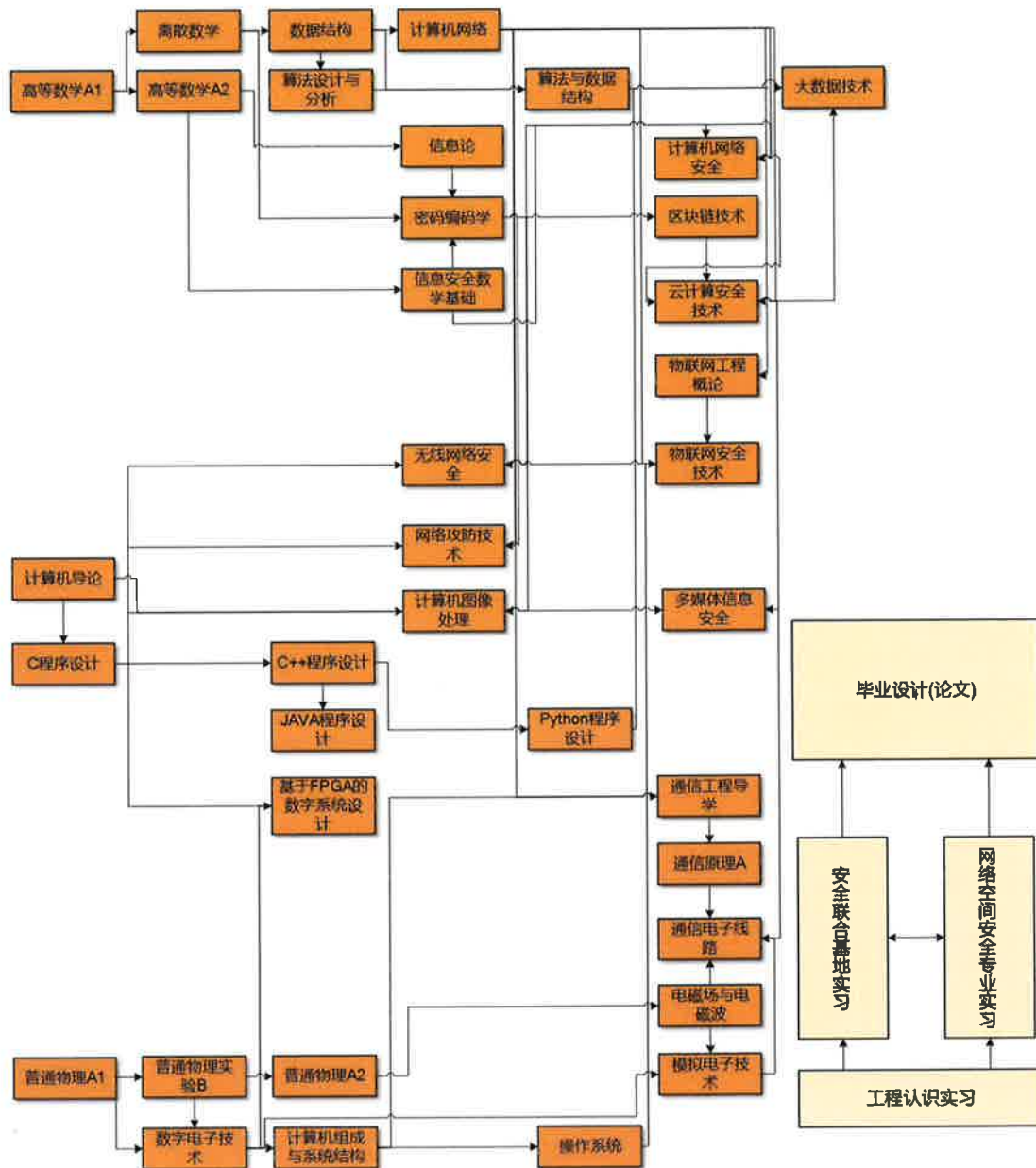
注：

- 1、本表待专业教学计划表中所有课程确定后再进行填写。
- 2、认证专业应确定课程支撑强度，用 H（高）、M（中）、L（弱）表示。
- 3、“课程”一行填写具体课程名称。
- 4、“毕业要求”一行仅需填写要求 1、要求 2，要求序号与培养方案中基本要求一致。

课程修读关系图



第1学期	第2学期	第3学期	第4学期	第5学期	第6学期	第7学期	第8学期
------	------	------	------	------	------	------	------



浙江理工大学网络空间安全新专业申报教学计划表

课程类别	课程性质	方向、模块、组名	课程名称	建议学年 学期	学分	总学时	分项学时			考试形式	考试方式
							讲课	实验	实践		
通识课	必修课		C 程序设计	一 1	2.0	32	32			集中	机试
			大学生心理健康教育	一 1	2.0	32	16	16			
			军事理论	二 1	2.0	36	21	15			
			高等数学 A1	一 1	6.0	96	96			集中	笔试
			普通物理 A1	一 1	3.0	48	48			集中	笔试
			高等数学 A2	一 2	5.0	80	80			集中	笔试
			普通物理 A2	二 1	3.0	48	48			集中	笔试
			职业发展与就业指导	三 1	2.0	38	16	22			
			劳动教育	一 2	1.0	16	16				
			创业基础	二 1	2.0	32	16	16			
			英语 2	一 1	3.0	48	48			集中	笔试
			英语 4	一 2	3.0	48	48			集中	笔试
			毛泽东思想和中国特色社会主义理论体系概论	二 1	3.0	48	40	8		集中	笔试
			习近平新时代中国特色社会主义思想概论	二 2	3.0	48	40	8		集中	笔试
			马克思主义基本原理	一 2	3.0	48	42	6		集中	笔试
			中国近现代史纲要	一 2	3.0	48	42	6		集中	笔试
			思想道德与法治	一 1	3.0	48	42	6		集中	笔试
			形势与政策	一 1	0.25	8	6	2			
			形势与政策	一 2	0.25	8	6	2			
			形势与政策	二 1	0.25	8	6	2			
			形势与政策	二 2	0.25	8	6	2			
			形势与政策	三 1	0.25	8	6	2			
			形势与政策	三 2	0.25	8	6	2			
			形势与政策	四 1	0.25	8	6	2			
			形势与政策	四 2	0.25	8	6	2			

	英语拓展课			要求修读英语拓展课至少 4 学分，详见英语拓展课课程组。									
	体育			要求修读体育课至少 4 学分，详见体育课程组。									
	选修课	要求修读通识选修课 14 学分，其中必须修读公共选修课 3 门（“四史”限定性选修课 1 门和艺术类限定性选修课 2 门），核心通识选修课在要求模块中至少选择 3 个模块的课程修读，其中限定修读“工程伦理与项目管理（60401）”，其他学分学生可在普通通识选修课中选择。											
学科 (专业) 基础课	必修课			计算机导论	— 2	1.0	16	16					
				离散数学	— 2	3.0	48	48			集中	笔试	
				数字电子技术	— 2	2.0	32	32					
				数据结构	二 1	3.0	48	48			集中	笔试	
				计算机组成与系统结构	二 1	2.0	32	32			集中	笔试	
				算法设计与分析	二 1	1.0	16	16					
				计算机网络	二 2	3.0	48	48			集中	笔试	
				操作系统	三 1	3.0	48	48			集中	笔试	
专业 课	必修课			信息论	三 1	3.0	48	48			集中	笔试	
				密码编码学	三 1	4.0	64	64			集中	笔试	
	选修课	非模块课	JAVA 程序设计	二 1	3.0	48	33	15					
			C++程序设计	二 1	3.0	48	33	15					
			算法与数据结构	二 2	3.0	48	33	15					
			信息安全数学基础	二 2	3.0	48	48						
			Python 程序设计	三 1	2.0	32	16	16					
			物联网安全技术	三 2	2.0	32	24	8					
			大数据技术	四 1	2.0	32	32						
			限定选修课	基于 FPGA 的数字系统设计	二 1	3.0	48	32	16				
		无线网络安全		二 2	2.0	32	32						
		网络攻防技术		二 2	2.0	32	32						
		计算机图像处理*		二 2	2.0	32	20	12					
		模块课	通信安全	通信电子线路	三 2	2.0	32	32					
				通信原理 A	三 2	2.0	32	24	8				
				电磁场与电磁波	三 2	3.0	48	48					
				模拟电子技术	三 2	2.0	32	32					

			通信工程导学*	三 2	2.0	32	32				
			物联网安全	三 2	2.0	32	32				
			计算机网络安全	三 2	2.0	32	32				
			多媒体信息安全	三 2	2.0	32	32				
			云计算安全技术*	三 2	2.0	32	32				
			物联网工程概论	三 2	2.0	32	32				
			区块链技术	三 2	2.0	32	32				
			要求在列出的专业选修课程中最低修读 28 学分，其中限定选修课必须修读 9 学分，学生应选择一个模块，并在选定模块中修读至少 8 学分，非模块课修至少读 11 学分。								
			身体素质课 1	三 1	0.5	8			8		
			身体素质课 2	三 2	0.5	8			8		
			社会实践	二 2	1.0	40			40		
			军事技能	一 1	2.0	40			40		
			普通物理实验 B	一 2	1.0	32		32			
			劳动教育实践	四 1	1.0	20			20		
			C 程序设计-实训	一 1	1.0	32			32		
			计算机组成与系统结构课程设计	二 1	1.0	20			20		
			毕业设计（论文）	四 2	8.0	320			320		
			程序设计基础课程设计	一 1	2.0	40			40		
			C++程序课程设计	二 1	1.0	20			20		
			大数据技术课程设计	四 1	1.0	20			20		
			操作系统课程实验	三 1	0.5	16		16			
			工程认识实习	二 1	1.0	20			20		
			网络空间安全专业实习	三 2	2.0	40			40		
			数据结构课程实验	二 1	1.0	32		32			
			安全联合基地实习	二 1	1.0	20			20		
			密码编码学综合实验	三 1	1.0	32		32			
			计算机网络课程设计	二 2	1.0	20			20		
			算法设计与分析实验	二 1	0.5	16		16			
			物联网安全技术课程设	三 2	1.0	20			20		
			信息论课程设计	三 1	2.0	40			40		

			无线网络安全课程设计	二 2	1.0	20			20		
			基于 FPGA 的数字系统设计实践	三 2	1.0	20			20		
			网络攻防技术实验	二 2	0.5	16		16			
	非模块课		Python 程序课程设计	三 1	1.0	20			20		
			Java 程序课程设计	二 1	1.0	20			20		
			算法与数据结构课程设计	二 2	2.0	40			40		
	模块课	通信安全	通信电子线路实验	三 2	0.5	16		16			
			通信原理课程设计	三 2	1.0	20			20		
			电磁场与电磁波实验	三 2	0.5	16		16			
		物联网安全	计算机网络安全实验	三 2	0.5	16		16			
物联网课程设计			三 2	1.0	20			20			
区块链技术课程设计			三 2	1.0	20			20			
要求在列出的实践选修课程中最低修读 10 学分，其中限定选修课必须修读，非模块选修课至少 3 学分，模块实践选修至少 1.5 学分。											

6. 教师及课程基本情况表

6.1 专业核心课程情况表

课程名称	课程总学时	课程周学时	拟授课教师	授课学期
信息论	48	3	沈剑	5
密码学编码学	64	4	周天祺、李全润	5
离散数学	48	3	严利平、高法钦	2
数据结构	48	3	王晨、谭皓文	3
计算机组成与系统结构	32	2	童基均、孔伟	3
计算机网络	48	3	金子龙、杨惠杰	4
操作系统	48	3	张一嘉、蒋路茸	5

6.2 本专业授课教师基本情况表

姓名	性别	出生年月	拟授课程	专业技术职务	学历	最后学历 毕业学校	最后学历 毕业专业	最后学历 毕业学位	研究领域	专职/兼职
沈剑	男	1985-01	信息论、 计算机导论	教授	研究生	韩国朝鲜大学	计算机工程	博士	网络空间安全	专职
童基均	男	1977-09	计算机组成与系统结构	教授	研究生	浙江大学	生物医学工程	博士	智能医学信息处理	专职
金子龙	男	1985-02	计算机网络、C++程序设计、 无线网络安全	教授	研究生	庆熙大学	计算机工学	博士	无线网络	专职
黄静	女	1965-05	通信原理A	教授	研究生	华中科技大学	电子科学与技术	博士	农业物联网应用	专职
严利平	女	1977-02	离散数学	教授	研究生	浙江理工大学	机械制造及其自动化	博士	信号与信息处理	专职
张一嘉	男	1981-08	操作系统、基于	教授	研究生	中国石油大学(华东)	控制理论与控制工	博士	通信对抗	专职

			FPGA的数字系统设计			)	程			
高法钦	男	1974-09	离散数学	副教授	研究生	北京航空航天大学	通信与信息系统	博士	智能信号处理	专职
蒋路茸	男	1982-07	操作系统	副教授	研究生	浙江大学	电路与系统	博士	物联网技术	专职
吴呈瑜	男	1982-11	电工电子技术基础	副教授	研究生	上海交通大学	通信与信息系统	博士	智能信号识别	专职
吴江	男	1978-05	通信工程导学	副教授	研究生	北京邮电大学	信号与信息处理	博士	无线通信	专职
戴燕云	女	1978-05	数字电子技术	副教授	研究生	浙江大学	电子科学与技术	博士	嵌入式电路与系统	专职
孔艳岩	女	1978-08	电磁场与电磁波	副教授	研究生	西南交通大学	通信与信息系统	博士	高功率微波源	专职
吕文涛	男	1982-09	通信原理A	副教授	研究生	上海交通大学	信息与通信工程	博士	嵌入式系统	专职
裘莹	男	1987-05	电磁场与电磁波、物联网工程概论	讲师	研究生	西北工业大学	计算机科学与技术	博士	工业物联网	专职
王晨	男	1994-04	数据结构、云计算安全技术	讲师	研究生	南京信息工程大学	信息与通信工程	博士	网络空间安全	专职
谭皓文	男	1991-08	数据结构、物联网安全技术	讲师	研究生	韩国	计算机工程	博士	网络空间安全	专职
周天祺	女	1994-04	密码编码学、计算机网络与信息安全	讲师	研究生	南京信息工程大学	信息安全	博士	公钥密码学	专职
李全润	男	1994-01	密码编码学、信息安全数学基础	讲师	研究生	武汉大学	网络空间安全	博士	应用密码学	专职
姜楠	男	1992-04	JAVA程序设计、计	讲师	研究生	美国内布拉斯加大	计算机工程	博士	网络和图像优化	专职

			计算机图像处理			学林肯分校				
杨惠杰	女	1995-01	计算机网络、算法设计与分析	讲师	研究生	南京信息工程大学	信息安全	博士	网络空间安全	专职
齐鹏嘉	女	1992-03	通信电子线路	讲师	研究生	吉林大学	微电子学与固体电子学	博士	嵌入式电路与系统	专职
曹天傲	男	1994-05	通信工程导学、计算机组成与系统结构	讲师	研究生	哈尔滨工业大学	仪器科学与技术	博士	智能医学信息处理	专职
佟威	男	1994-03	Python程序设计、区块链技术	讲师	研究生	西安电子科技大学	网络空间安全	博士	网络空间安全	专职
孔伟	男	1995-11	计算机组成与系统结构、大数据技术、网络攻防技术	讲师	研究生	中国人民解放军军事科学院	计算机科学与技术	博士	人工智能安全	专职
王雨佳	女	1991-05	多媒体信息安全	讲师	研究生	北京理工大学	计算机科学与技术	博士	人机交互/多媒体	专职
李鑫成	男	1995-01	算法与数据结构	助教	研究生	扬州大学	软件工程	博士	信息安全	专职

6.3教师及开课情况汇总表

专任教师总数	26		
具有教授（含其他正高级）职称教师数	6	比例	23.08%
具有副教授及以上（含其他副高级）职称教师数	13	比例	50.00%
具有硕士及以上学位教师数	26	比例	100.00%
具有博士学位教师数	26	比例	100.00%
35岁及以下青年教师数	12	比例	46.15%

36-55岁教师数	13	比例	50.00%
兼职/专职教师比例	0:26		
专业核心课程门数	7		
专业核心课程任课教师数	13		

7. 专业主要带头人简介

姓名	沈剑	性别	男	专业技术职务	教授	行政职务	院长
拟承担课程	计算机导论、信息论			现在所在单位	浙江理工大学		
最后学历毕业时间、学校、专业		2012年毕业于韩国朝鲜大学情报与通信专业					
主要研究方向		网络空间安全、区块链、云计算安全					
从事教育教学改革研究及获奖情况（含教改项目、研究论文、慕课、教材等）		承担《密码编码学与网络安全》等课程，入选省级外国留学生英语授课精品课程。已完整培养过博士生3人，硕士生26人					
从事科学研究及获奖情况		主持国家重点研发计划、国家自然科学基金联合重点项目等国家重大重点项目3项，入选浙江省领军型创新团队。牵头获教育部自然科学二等奖、中国密码学会优秀青年奖、江苏省计算机学会青年科技奖等奖励。在IEEE TDSC、TIFS等期刊/会议上发表论文百余篇，其中CCFA类论文12篇，ESI高被引论文9篇					
近三年获得教学研究经费（万元）	36.7			近三年获得科学研究经费（万元）	330.0		
近三年给本科生授课课程及学时数	授课密码编码学与网络安全课程学时160			近三年指导本科毕业设计（人次）	24		

姓名	童基均	性别	男	专业技术职务	教授	行政职务	无
拟承担课程	计算机组成与系统结构			现在所在单位	浙江理工大学		
最后学历毕业时间、学校、专业	2008毕业于浙江大学生物医学工程						
主要研究方向	医院信息化与医疗大数据、智能医学信息处理、视频信息处理、脑机接口						
从事教育教学改革研究及获奖情况（含教改项目	承担单片机原理与应用、智能穿戴设备与物联网技术等课程的教学工作						

、研究论文、慕课、教材等)							
从事科学研究及获奖情况		主持国家自然科学基金、浙江省重点研发计划项目、浙江省自然科学基金等项目，专利转化及应用取得经济效益500万元以上。近5年发表SCI、EI学术论文数37篇，授权发明专利6项和4项软件著作权，指导研究生获奖3项。中国电子学会高级会员，浙江省电子学会理事					
近三年获得教学研究经费（万元）	6.0			近三年获得科学研究经费（万元）	262.0		
近三年给本科生授课课程及学时数	授课智能穿戴设备与物联网技术课程学时48，授课单片机原理与应用课程学时32，授课单片机课程设计课程学时20			近三年指导本科毕业设计（人次）	12		
姓名	张一嘉	性别	男	专业技术职务	其他正高级	行政职务	无
拟承担课程	操作系统、基于FPGA的数字系统设计			现在所在单位	浙江理工大学		
最后学历毕业时间、学校、专业		2014毕业于中国石油大学（华东）控制理论与控制工程					
主要研究方向		通信对抗、软件无线电和复杂网络					
从事教育教学改革研究及获奖情况（含教改项目、研究论文、慕课、教材等）		承担通信原理、数学建模与分析等课程的教学工作					
从事科学研究及获奖情况		主持国家863计划、国防预研项目、集团创新项目和国防型研项目，累计科研经费1500余万。近5年发表论文14篇，其中SCI/EI检索10篇。获中国人民解放军总装备部科技进步奖一等奖、中国电子科技集团公司科学技术奖一等奖和中国电子科技集团公司科学技术奖三等奖一项和中国电子科技集团公司第三十六所首届科技贡献奖。现为中国电子科技集团公司集团专家、通信系统信息控制技术国家级重点实验室/战术互联网DK室主任					
近三年获得教学研究经费（万元）	6.0			近三年获得科学研究经费（万元）	185.5		
近三年给本	授课通信原理课程学时48，授课数学			近三年指导	7		

科生授课课程及学时数	建模与分析课程学时32			本科毕业设计（人次）			
姓名	金子龙	性别	男	专业技术职务	教授	行政职务	副院长
拟承担课程	计算机网络、C++程序设计、无线网络安全			现在所在单位	浙江理工大学		
最后学历毕业时间、学校、专业		2016毕业于庆熙大学计算机工学					
主要研究方向		无线网络，物联网安全					
从事教育教学改革研究及获奖情况（含教改项目、研究论文、慕课、教材等）		“基于海量标签和压缩编码的无源感知平台”，中国发明学会，发明创业奖创新奖二等奖，2021年11月，国科奖社证字第0123号					
从事科学研究及获奖情况		完成了韩国科学部项目“A Study on East-West Neo-Medical u-Life Care Technology”，军委科技委“173”国防基础加强项目“复杂**敏捷构建与新理论与关键技术研究”，国家自然科学基金青年基金项目“认知无线电传感器网络中能耗优化的智能通信算法研究”等5项，发表论文40余篇、其中SCI论文10余篇，授权发明专利10余件。目前正在主持国家自然科学基金面上项目“面向空、地协同边缘网络的智能自治网络关键技术研究”、浙江省“尖兵领雁”重大科技计划项目“商用密码和信息技术创新（信创）技术研究及应用”。兼任韩国网络学会SCI期刊“Transaction on Internet and Information Systems”领域编辑					
近三年获得教学研究经费（万元）	5.0			近三年获得科学研究经费（万元）	454.0		
近三年给本科生授课课程及学时数	C++程序设计（96学时），数据库安全（48学时），计算机网络（96学时）			近三年指导本科毕业设计（人次）	10		

8. 教学条件情况表

可用于该专业的教学实验设备总价值（万元）	588.06	可用于该专业的教学实验设备数量（千元以上）	135（台/件）
开办经费及来源	本专业开办经费在原有数字时尚与数据治理重点实验室等六个教学基地的相关实验设备135件(千元以上)，总经费588.063万的基础上，将得到学校、学院以及上级财政等总计270万的建设经费支持，具体如下：学科经费100万元，用于专业建设相关投入；上级财政新设备购置经费140万元，保障实验室设备更新补充；学校支持新专业建设经费30万元，助力教学条件完善等工作。		
生均年教学日常运行支出（元）	1200.0		
实践教学基地（个）	4		
教学条件建设规划及保障措施	教学条件建设规划：信息科学与工程学院计划将浙江理工大学21号楼作为网络空间安全专业的教学与科研主楼，并进一步建设数字时尚与数据治理省重点实验室。 教学保障措施：学院一贯注重教学管理，注重教学质量监控和评估，不断完善教学督导、考场巡查、学生评教、教学检查等教学监督与反馈制度，不断完善教学质量保障体系，全面提升专业教师教学水平和人才培养质量。坚持实施三阶段检查制度、加强教学信息员学生管理、实施周报月报相结合的质量监控体系，在促进教学改革等方面充分发挥教学督导评价和指导作用。规范管理，严格要求，狠抓教学质量。根据全国各地学生的高数和英语基础，实施分层教学，培优补差。学院还将成立专业建设指导委员会，聘请各专业的行业、企业、兄弟高校的专家参与专业建设、实训基地建设的研讨和论证。确保人才培养方案、课题体系、实训基地方案的科学性、可行性。		

主要教学实验设备情况表

教学实验设备名称	型号规格	数量	购入时间	设备价值（千元）
服务器	富士通F250	1	2003	51.0
惠普服务器	DL388G10	4	2019	35.0
交换机	H3C	13	2019	1.0
核心交换机	H3C	1	2019	25.0
联想台式电脑	启天M425、19.5*	90	2019	5.0
东软防火墙	FW5120-D2110	2	2019	12.0

投影机	NEC ME360XC	2	2012	8.0
服务器机柜	IBM42U	1	2009	10.0
路由器	H3C SMB-ER6300-CN	2	2012	5.0
工控安全实验箱	V1.0	6	2025	100.0
安全模块装置	V1.0	5	2025	60.0
竞赛实训装置	V1.0	1	2025	630.0
应急演练实训装置	V1.0	1	2025	650.0
火力发电网络安全演练 沙盘	V1.0	1	2025	400.0
红蓝对抗实训装置	V1.0	1	2025	825.0
行业攻防展架	V1.0	1	2025	400.0
试验鉴定装置	V1.0	1	2025	675.0
工控安全实验柜	V1.0	1	2025	500.0

9. 申请增设专业的理由和基础

一、申请新增专业主要理由

全球对网络空间安全的要求越来越高，网络空间安全作为非传统安全因素，已与各国的政治安全、经济安全、国防安全和文化安全共同成为国家安全的重要组成部分。网络空间安全是关乎国家安全和发展的重大战略问题，我国一贯高度重视。早在 2003 年，就颁发了《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发〔2003〕27 号文件）。2013 年 11 月 12 日成立中央国家安全委员会。2014 年 2 月 27 日成立中央网络安全和信息化领导小组，同时，“维护网络安全”首次列入政府工作报告。国家《国民经济和社会发展第十四个五年规划和 2035 年远景目标纲要》中明确提出，要全面加强网络安全保障体系和能力建设，加强网络安全宣传教育和人才培养。

1、国防建设对网络空间安全高层次人才的需求

信息对抗与攻防能力已成为重要的国防力量之一。美国很早就提出了信息战的概念，在海湾战争期间美军成功地对伊拉克发动了信息战。2009 年 6 月正式成立美军的网络司令部，大批接收网络安全的专门人才组建网络空间安全作战部队。我军要打赢信息化条件下的局部战争，提高基于信息系统的体系作战能力，关键是要有一支专门的网络与信息安全人才队伍。2014 年，习近平在中央网络安全和信息化领导小组第一次会议上的讲话指出“没有网络安全就没有国家安全”。10 月，经习近平主席批准，中央军委印发了《关于进一步加强军队信息安全工作的意见》。《意见》中明确强调了“扎实抓好信息安全防护力量建设，为信息安全建设管理提供人才支撑”。2022 年国家计算机病毒应急处理中心和 360 公司分别发布了关于西北工业大学遭受境外网络攻击的调查报告。调查发现，网络攻击来自美国国家安全局（NSA）下属的特定入侵行动办公室（TAO），使用了 41 种不同的专属网络攻击武器，持续对西北工业大学开展攻击窃密。党的二十大报告进一步指出“提高公共安全治理水平，加强个人信息保护”，这对网络空间安全相关专业领域的建设和人才的培养提出了更高的要求。

2、国家互联网经济建设对网络空间安全高层次人才的需求

据 2022 年的《中国互联网络发展状况统计报告》显示，互联网推动网民消

费模式变迁，2015 年 12 月我国网络支付用户规模达 4.16 亿，截止 2022 年 6 月我国网络支付用户规模达 9.04 亿。互联网提供大量免费内容服务及信息服务，促使以流量、时间消费为特点的新型消费快速增长，从 2001 年 12 月到 2022 年 6 月，我国网民每周上网时长从 8.5 小时增长至 29.5 小时，互联网与人们生产生活结合日益紧密，网络与信息技术已经成为当前互联网消费的主要动力。消费模式的变迁同样带来巨大的挑战，对信息的安全性、保密性、可用性等提出较高的要求。网络空间安全方面最主要的安全威胁来自安全漏洞，其中又以未公开漏洞为主要威胁。2014 年，著名的 heart-bleed 漏洞在被披露前，长期被黑客利用，窃取大量互联网用户隐私信息，而 2017 年初爆发的 wannacry 勒索病毒，也正是由不法分子利用 NSA（美国国家安全局）泄露的危险漏洞“EternalBlue（永恒之蓝）”进行传播。据统计 2022 年我国遭遇个人信息泄露、网络诈骗、病毒或木马的网民比例超 48%，其中以信息平台为基础的虚拟中奖信息诈骗、网络购物诈骗等超过了网络诈骗问题的 70%，可见信息的安全形势非常严峻。截至 2022 年 6 月，仍有 36.8%的网民表示过去半年在上网过程中遭遇过网络安全问题。特别是 2020 年新冠肺炎疫情爆发以来，随着网络支付与无接触支付越来越普及，信息技术成为重要安全保障。国家的网络强国建设、国民新型消费都需要一支掌握网络空间安全专业知识的团队。

3、网络空间安全产业的发展对高层次人才的需求

随着互联网和信息技术的飞速发展，网络空间安全问题也日益凸显，市场需求十分旺盛。IDC 数据显示，2021 年全球网络安全相关硬件、软件、服务总投资规模达到 1687.7 亿美元，预计在 2026 年增至 2875.7 亿美元，五年复合增长率（CAGR）将达 11.3%。聚焦中国市场，2026 年中国网络安全 IT 支出规模将达到 318.6 亿美元，全球占比约为 11.1%，五年 CAGR 约为 21.2%。中国网络安全市场增速持续领跑全球，五年 CAGR 近全球两倍，市场前景广阔。伴随云计算的快速发展，中国网络安全市场的信息化趋势在不断增强。未来五年，社会对信息安全的人才需要量大约为每年增加 1.2 万人左右。在“十四五”规划下，未来五年信息安全市场会跟随国家整体科技进步的方向快速发展，随着网络空间安全占据市场越来越大，对于网络空间安全专门人才需求量急剧增加。据《网络安全

人才实战能力白皮书》，我国此类专业人才缺口超过 140 万，缺口高达 95%。而每年高校安全专业培养人才仅有三万余人，预计 2027 年缺口将进一步扩大到 300 万。总体来说，目前网络空间安全专业领域的人才培养极度匮乏、刻不容缓。

网络空间安全专业毕业生经过四年的学习可以满足国家战略需求，就业领域包括以下几个方面：

1) 可从事安全信息服务：为政府、国防、军队、电信、电力、金融、铁路等部门的网络与信息安全领域进行管理、科研与服务；

2) 可从事安全技术研发：到国内外大型电信服务商、大型通信设备制造企业、国内外众多软件企业、国家机关以及各个大中型企事业单位的信息技术部门、教育部门进行安全技术的研究、设计、开发、维护和教育培训等工作；

3) 可继续网络空间安全深造：继续攻读计算机科学与技术、信息安全、网络工程、通信、信息处理、软件工程和其他相关学科的硕士学位。

二、现有学科基础

1. 学科基础

当前，网络空间安全学科依托通信工程专业培养体系的建设展开，开设了《计算机网络与信息安全》专业必修课，并在通信工程下设置网络空间安全专业方向，开设了《密码编码学》《无线网络安全技术》《云计算安全技术》《区块链技术》《数据库原理及安全》《多媒体信息安全》等专业选修课。注重培养学生的网络空间安全专业方面基础理论、基本知识、基本技能和相关学科知识，具有在网络空间安全领域进行设计开发、优化和应用的能力，有较强的专业实践和创新能力，能够在网络空间安全及其相关领域从事信息安全产品研发、网络安全体系规划、防御、运维和管理等工作的网络空间安全专业人才。

2. 人才培养

学院通过“本科生导师制”、“竞赛培训班”等多种方式在科学研究、创新创业方面激发学生在网络空间安全、网络攻防等方面的兴趣、提高学生动手实践能力。产教融合构建实践教学体系，加强专业建设，积极组织学生参加全国大学生

网络空间安全竞赛等相关学科竞赛。

培养学生获本科生省优秀毕业设计、省优硕等；获国家级竞赛一等奖 54 项、二等奖 113 项、三等奖 146 项，获省级竞赛一等奖 123 项、二等奖 170 项、三等奖 263 项，其中获全国大学生网络空间安全竞赛国赛特等奖 1 项、三等奖 1 项，浙江省大学生网络与信息安全竞赛一等奖 22 项，美国大学生数学建模竞赛特等奖 1 项。

《密码编码学与网络安全》课程入选省级外国留学生英语授课精品课程，获省级研究生教育改革成果奖一等奖，《云辅助下的智能网络数据安全保护与应用技术》省级教育教学与研究成果奖二等奖（排名第一），《新网络环境下的多媒体内容应用与安全保护技术》省级教育教学研究成果奖三等奖。参与编写《大数据、数据挖掘及应用实践》等教材/专著 4 本。

获批“产教融合《计算机网络与信息安全》课程建设研究”等教育部产学研合作协同育人项目 6 项，“新工科背景下面向行业需求的网络空间安全课程群建设”浙江省产学研合作协同育人项目 1 项。获批工信部教育与考试中心“信息技术应用创新人才培养与评价基地”。

3. 师资队伍

开展“青蓝工程”，经验丰富老教师通过“传、帮、带”促进青年教师快速成长，明确“立德树人”根本任务。现拥有一支年富力强、结构合理的教师队伍，入选网安领域国家“万人计划”科技创新领军人才 2 人，入选浙江省“分布式异构数据安全与隐私保护”领军型创新团队，引进网安相关人才 10 余人。

4. 科学研究

建有全省数字时尚与数据治理重点实验室、云计算安全与数据聚合省国际科技合作基地、智能软件安全分析与可靠性测试省国际联合实验室，与海康威视共建全省智能物联网与数据安全重点实验室。与海康威视、安恒信息共建了“多媒体大数据安全”、“云计算安全”联合实验室，与加拿大温莎大学、丹麦科技大学共建云计算与网络安全、人工智能与物联网安全国际联合实验室，与挪威奥斯陆大学、新加坡管理大学等 7 所国际知名高校签署战略合作协议，围绕“云计算

安全”、“网络与数字孪生安全”、“人工智能安全”等主题展开长期合作研究。牵头主持相关国家级项目 19 项，其中包括国家重点研发计划“区块链”重点专项、国家自然科学基金委联合重点项目等国家重大重点项目 4 项，主持相关省部级项目 22 项；获教育部自然科学二等奖（排名第一）、浙江省科技进步奖等科技奖励 5 项；发表高水平论文 250 余篇，高被引论文 19 篇。

先后承办中国密码学会等国内一级学会学术年会 3 次，教育部主办 2023 先进材料与智能制造国际产学研用合作会议大数据安全与智能制造分论坛、网络安全国际研讨会（CS2024）、区块链与可信系统国际会议（BlockSys'2024）等国际会议，具有较好的国际国内影响力。

三、与学校专业学科发展规划的适配度

随着网络空间安全上升为国家战略，网络空间安全专业的发展迎来了新的机遇。《浙江理工大学“十四五”学科建设实施方案》指出要“强化学科内涵建设”，按照“强化优势、突出特色、交叉融合、协调发展”的总体原则，加快培育新兴学科，“大数据与信息安全”是浙江省“315”科创体系建设工程十五大战略领域之一，网络空间安全相关学科也是国家学科专业体系建设的急需学科，网络空间安全专业的设立能够增强学校在科技领域尤其是在信息技术领域的研究和教育能力。该专业不仅能提升学校在网络安全、加密技术等前沿领域的科研水平，还能满足国家对高水平网络空间安全人才的迫切需求。通过与通信工程、电子信息工程等现有学科的互补和协同，网络空间安全专业将促进跨学科课程和联合科研项目的发展，丰富学校的人才培养体系，为学生提供更多专业选择和发展路径。通过引入网络空间安全专业，学校将进一步增强信息工科的综合实力和学术影响力。

网络空间安全专业的设立与学校的专业学科发展规划高度契合，能够响应国家战略，支持学校软件工程、信息与通信工程、计算机科学与技术、网络空间安全等学科发展，提升科技创新与科研水平，满足社会人才需求。

10. 校内专业设置评议专家组意见表

校内专业设置评议专家组意见表

总体判断拟开设专业是否可行		☒ 是 ☐ 否
理由： 习近平总书记在全国网络安全和信息化工作会议上明确指出，“没有网络安全就没有国家安全，就没有经济社会稳定运行，广大人民群众利益也难以得到保障”。网络空间安全已成为国家安全的重要组成部分，是国家安全对抗的主战场。教育部《加强网络安全学科建设和人才培养的意见》指出要“支持网络安全学院学科专业建设，加快网络安全人才培养，为实施网络强国战略、维护国家网络安全提供强大的人才保障”。网络空间安全专业的设立高度契合国家总体安全观和数字化发展战略，网络空间安全人才培养是保障网络空间治理、国家安全对抗的关键。“大数据与信息安全”是浙江省“315”科创体系中的十五大战略领域之一，对网络空间安全人才需求迫切。 我校增设网络空间安全专业，契合国家发展战略，推动浙江省数字经济发展，符合学校发展总体定位。 网络空间安全专业规划清晰，培养方案目标明确，课程设置合理，专业特色鲜明。师资职称、年龄、学缘结构合理。网络空间安全专业将依托信息与通信工程一级学科硕士点、电子信息(网络与信息安全)专业学位硕士点、全省数字时尚与数据治理重点实验室、全省智能物联网与数据安全重点实验室、云计算安全与数据聚合省国际科技合作基地、工信部信息技术应用创新人才培养与评价基地、信息电子省级实验教学示范中心、无线传感与智能感知省级重点实验教学示范中心，与企业展开深度合作，深化产教融合和协同育人。学校将通过专业建设、实验室建设、校外实践基地建设等渠道，统筹经费分配，给予新专业建设以充足的经费保障和政策支持。 综上，同意上报网络空间安全专业。		
拟招生人数与人才需求预测是否匹配		☒ 是 ☐ 否
本专业开设的基本条件是否符合教学质量国家标准	教师队伍	☒ 是 ☐ 否
	实践条件	☒ 是 ☐ 否
	经费保障	☒ 是 ☐ 否
专家签字： 